



SOLUTION BRIEF

Industrial Defender for Splunk App: Investigate Security Events with Deep Contextual Data

When a security event occurs in complex operational technology (OT) environments, it can be difficult to get the right information to the right people to quickly respond to an emerging cybersecurity threat. Industrial Defender for Splunk app solves this challenge by delivering security events with deep asset context to analysts, so they can quickly identify and mitigate potential cybersecurity issues.

The app increases the effectiveness of using Splunk in OT environments by providing not just alert data, but also contextual asset information including location, criticality, and contact information for the OT asset owner. Industrial Defender API Add-on for Splunk also eliminates the manual process of mapping the comprehensive data sets provided by Industrial Defender to the Splunk user interface.

Industrial Defender for Splunk Benefits

- Detect recent changes and security events across your asset base and at your perimeter to take decisive action when vulnerabilities and threats are identified.
- Mitigate cyberthreats quickly with actionable, contextual security event data.
- Enhance IT and OT collaboration with common situational awareness into critical ICS environments.
- Quickly access asset data like location, criticality, and contact information for the OT asset owner in Splunk.

[INDUSTRIALDEFENDER.COM](https://www.industrialdefender.com)



SOLUTION COMPONENTS

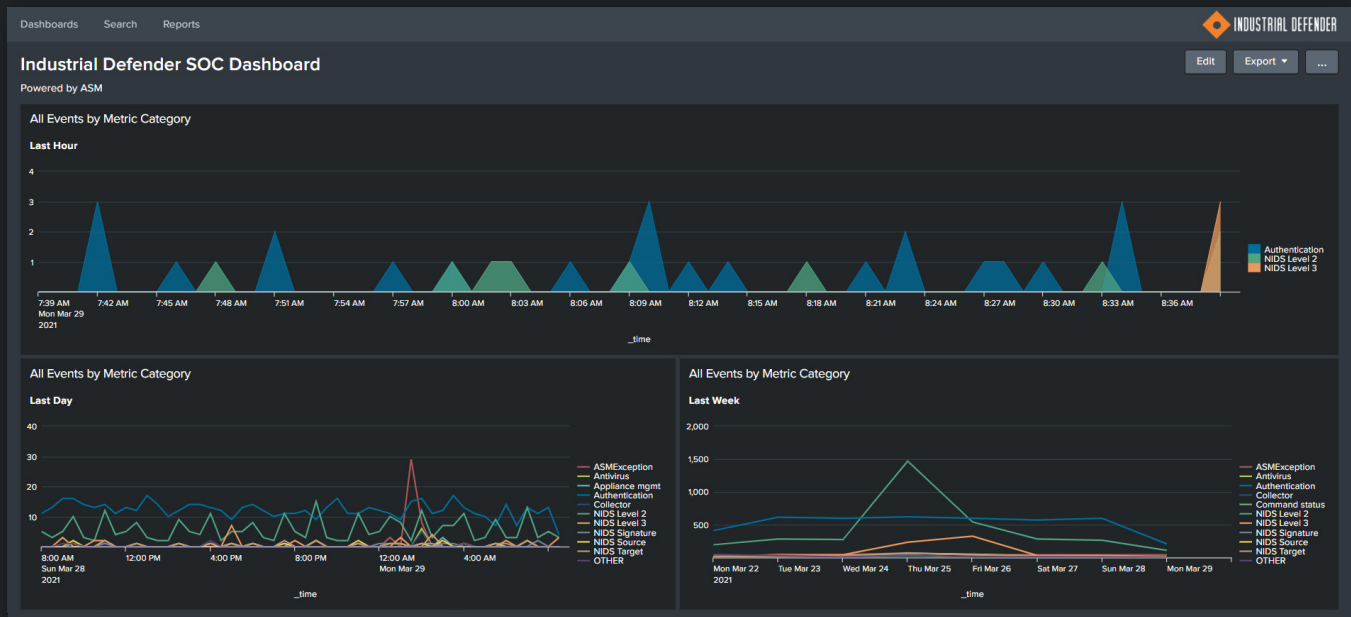
- Industrial Defender for Splunk
- Industrial Defender API Add-on for Splunk

Use Cases

Industrial Defender for Splunk App delivers contextual asset and network data related to security events and changes into two pre-configured dashboards, the SOC Dashboard and the Asset Insights Dashboard. Having this actionable data at their fingertips helps security teams reduce the mean time to respond (MTTR) to a potential cybersecurity threat in critical OT environments.

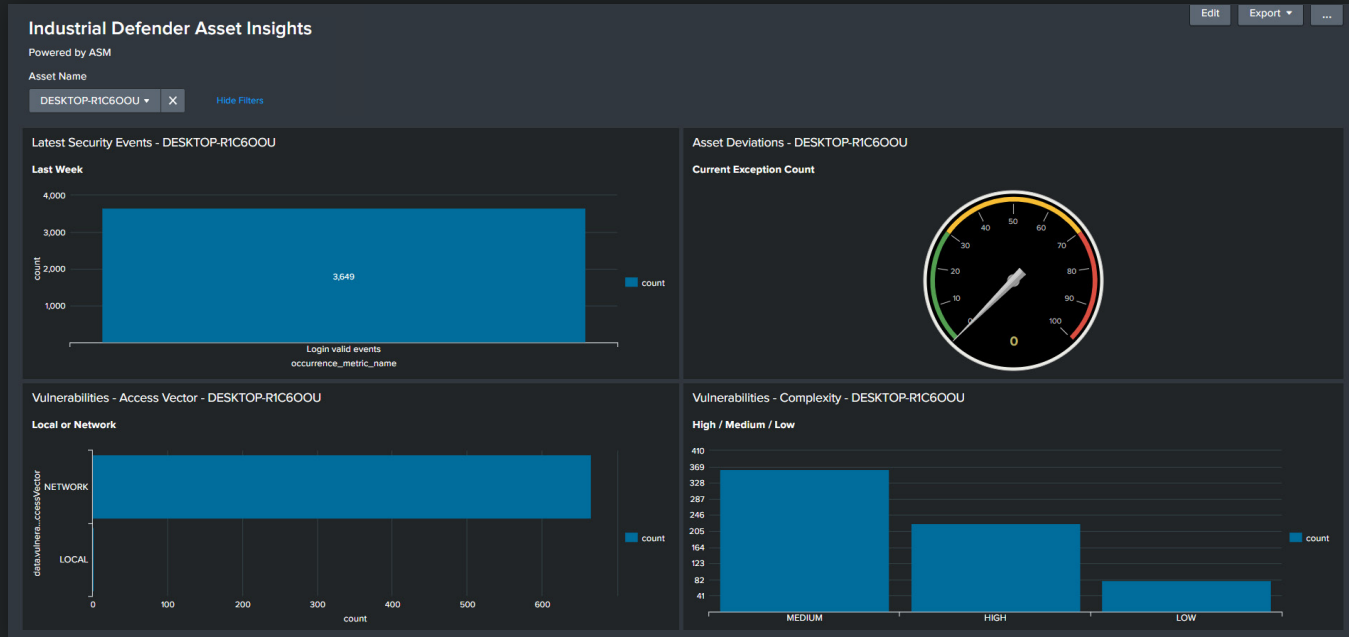
SOC DASHBOARD

Monitor OT security events by category



ASSET INSIGHTS DASHBOARD

Monitor OT security events, administrative properties, baseline deviations, and vulnerabilities



Asset Properties - DESKTOP-01KH57B

Administrative Properties

Property Name	Property Value
Criticality	Low
Acid	No
IDef_Host Type	Agent
Asset Model Type	Windows
Asset Model	Virtual
IDef_SEM Location	none
Address 1	225 Foxborough Blvd
Address 2	Suite 202
City	Foxboro
State/Province	MA

Software Deviations - DESKTOP-01KH57B

Current Exceptions

Application	Version	Date
C:\Users\All Users\Microsoft\Windows Defender\Definition Updates\StableEngineEtWLocation\Wpengine_etw.dll	1.1.17800.5	2021-02-02T07:28
C:\Users\All Users\Microsoft\Windows Defender\Definition Updates\{8E58618C-F410-4497-A271-66248F94F585}\Wpengine.dll	1.1.17800.5	2021-02-16T07:21
C:\Users\All Users\Microsoft\Windows Defender\Platform\4.18.2010.7-0\Config\SecurityPolicy.exe	4.18.2010.7	2020-12-08T13:09
C:\Users\All Users\Microsoft\Windows Defender\Platform\4.18.2010.7-0\DefenderCSP.dll	4.18.2010.7	2020-12-08T13:09
C:\Users\All Users\Microsoft\Windows Defender\Platform\4.18.2010.7-0\WpAsDesc.dll	4.18.1901.16384	2020-12-08T13:09
C:\Users\All Users\Microsoft\Windows Defender\Platform\4.18.2010.7-0\WpAzSubmit.dll	4.18.2010.7	2020-12-08T13:09
C:\Users\All Users\Microsoft\Windows Defender\Platform\4.18.2010.7-0\WpClient.dll	4.18.2010.7	2020-12-08T13:09
C:\Users\All Users\Microsoft\Windows Defender\Platform\4.18.2010.7-0\WpCmdRun.exe	4.18.2010.7	2020-12-08T13:09
C:\Users\All Users\Microsoft\Windows Defender\Platform\4.18.2010.7-0\WpCommu.dll	4.18.2010.7	2020-12-08T13:09
C:\Users\All Users\Microsoft\Windows Defender\Platform\4.18.2010.7-0\WpDetours.dll	4.18.2010.7	2020-12-08T13:09

Software Patch Deviations - DESKTOP-01KH57B

Current Exceptions

Patch	Date	Type
KB4502496	2021-01-13T01:56:03Z	New Actual
KB4535684	2021-01-13T01:56:03Z	New Actual
KB4535685	2021-01-13T01:56:03Z	New Actual
KB4580980	2020-11-14T01:45:09Z	New Actual
KB4535680	2021-01-13T01:56:03Z	New Actual
KB4577670	2020-10-17T00:57:09Z	New Actual
KB4580325	2020-10-17T00:57:09Z	New Actual
KB4584229	2020-11-14T01:45:09Z	New Actual
KB4586863	2020-11-13T15:04:59Z	New Actual
KB4586878	2021-01-13T01:56:03Z	New Actual

User Account Deviations - DESKTOP-01KH57B

Current Exceptions

UserID	UserType	Enabled	Date	Type
Access Control Assistance Operators	null	true	2020-12-08T10:00:10Z	New Actual
Administrators	null	true	2020-12-08T10:00:10Z	New Actual
Backup Operators	null	true	2020-12-08T10:00:10Z	New Actual
Cryptographic Operators	null	true	2020-12-08T10:00:10Z	New Actual
Device Owners	null	true	2020-12-08T10:00:10Z	New Actual
Distributed COM Users	null	true	2020-12-08T10:00:10Z	New Actual
Event Log Readers	null	true	2020-12-08T10:00:10Z	New Actual
Guests	null	true	2020-12-08T10:00:10Z	New Actual
Hyper-V Administrators	null	true	2020-12-08T10:00:10Z	New Actual
IIS_IUSRS	null	true	2020-12-08T10:00:10Z	New Actual

Asset Detail Deviations - DESKTOP-01KH57B				Firewall Rule Deviations - DESKTOP-01KH57B						Port & Service Deviations - DESKTOP-01KH57B				
Current Exceptions				Current Exceptions						Current Exceptions				
Attribute	Value	Date	Type	srcAddr	destAddr	Service	Status	Date	Type	Port	Protocol	Process	Date	Type
Time Zone Offset	-480 minutes	2020-11-13T15:04:50Z	Changed Actual	any	internal	Local: 1900 Remote: 5357	disabled	2020-10-15T19:48:57Z	Changed Actual	135	TCP	svchost.exe[RpcEptMapper]	2020-12-09T10:00:33Z	New Actual
				any	internal	Local: 2869 Remote: 2869	disabled	2020-10-15T19:48:57Z	Changed Actual	135	TCP	svchost.exe[RpcSs]	2020-12-09T10:00:33Z	New Actual
				any	internal	Local: 5353 5800-5020 Remote: 80,443 8554-8558	enabled	2020-11-14T01:45:09Z	New Actual	1900	UDP	svchost.exe[SSDPSRV]	2021-01-13T10:00:26Z	New Actual
				any	internal	Local: 5353 5800-5020 Remote: 80,443 8554-8558	enabled	2021-02-02T07:28:33Z	New Actual	3389	UDP	svchost.exe[TermService]	2020-12-09T10:00:33Z	New Actual
				any	internal	Local: 5353 5800-5020 Remote: 80,443 8554-8558	enabled	2021-02-02T07:28:33Z	New Actual	3782	UDP	svchost.exe[DResPub]	2021-01-29T13:30:56Z	New Actual
				internal	any	Local: 5353 5800-5020 Remote: 80,443 8554-8558	enabled	2021-02-02T07:28:33Z	New Actual	4500	UDP	svchost.exe[IREEXT]	2021-01-29T13:30:56Z	New Actual
										49666	TCP	svchost.exe[EventLog]	2021-02-02T07:28:33Z	New Actual
										49667	TCP	svchost.exe[Schedule]	2021-02-02T07:28:33Z	New Actual
										49668	TCP	svchost.exe[SessionEnv]	2021-01-13T01:56:03Z	New Actual
										49670	TCP	services.exe	2021-01-29T13:30:56Z	New Actual

Vulnerabilities - DESKTOP-R1C600U				
ID	CVSScore	Complexity	Vector	Summary
CVE-2016-3201	4.3	MEDIUM	NETWORK	Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold and 1511, and Microsoft Edge allow remote attackers to obtain sensitive information from process memory via a crafted PDF document, aka "Windows PDF Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3215.
CVE-2016-3215	4.3	MEDIUM	NETWORK	Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 1511, and Microsoft Edge allow remote attackers to obtain sensitive information from process memory via a crafted PDF document, aka "Windows PDF Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3201.
CVE-2016-3370	4.3	MEDIUM	NETWORK	The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka "PDF Library Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3374.
CVE-2016-3374	4.3	MEDIUM	NETWORK	The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka "PDF Library Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3370.
CVE-2020-1350	10.0	LOW	NETWORK	A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests, aka "Windows DNS Server Remote Code Execution Vulnerability".
CVE-2016-0841	7.2	LOW	LOCAL	CVE-426: Untrusted Search Path/a>
CVE-2016-0859	4.3	MEDIUM	NETWORK	The Hyperlink Object Library in Microsoft Internet Explorer 9 through 11 allows remote attackers to obtain sensitive information from process memory via a crafted URL in a (1) e-mail message or (2) Office document, aka "Internet Explorer Information Disclosure Vulnerability."
CVE-2016-0860	9.3	MEDIUM	NETWORK	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0861, CVE-2016-0863, CVE-2016-0867, and CVE-2016-0872.
CVE-2016-0861	9.3	MEDIUM	NETWORK	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0860, CVE-2016-0863, CVE-2016-0867, and CVE-2016-0872.
CVE-2016-0862	9.3	MEDIUM	NETWORK	Microsoft Internet Explorer 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."



ABOUT INDUSTRIAL DEFENDER:

Since 2006, Industrial Defender has been solving the challenge of safely collecting, monitoring, and managing OT asset data at scale, while providing cross-functional teams with a unified view of security. Their specialized solution is tailored to complex industrial control system environments by engineers with decades of hands-on OT experience. Easy integrations into the broader security and enterprise ecosystem empower IT teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks. Learn more at www.industrialdefender.com.

SCHEDULE A DEMO

FOR MORE INFORMATION

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com
 225 Foxborough Blvd, Foxborough, MA 02035
industrialdefender.com

© 2021 iDefender, LLC